3rd Annual Cross-Domain Deterrence Seminar: Towards Integrated Strategic Deterrence

Summary Report

November 15-17, 2016

CGSR
Center for Global Security Research

National Security Office
Lawrence Livermore National Laboratory

LLNL-TR-72737

3rd Annual Cross-Domain Deterrence Seminar

Author: Eric Jacobson
Graduate Student Researcher, Center for Global Security Research, LLNL
Masters in International Affairs, School of International and Public Affairs, Columbia University, 2016

Lawrence Livermore National Laboratory (LLNL) hosted the 3rd Annual Cross-Domain Deterrence (CDD) Seminar on November 15-17, 2016 in Livermore, CA. The seminar was sponsored by LLNL's National Security Office (NSO) and Center for Global Security Research (CGSR). The primary purpose of the seminar was to utilize the cross-domain framework to work toward an approach for comprehensive and integrated strategic deterrence. The seminar focused on a tabletop exercise (TTX) to explore the dynamics of escalation and de-escalation in cyber space, outer space, and the nuclear domain. The TTX explored a scenario involving a NATO Article V defense of a Baltic ally. To help inform game "play," the exercise was preceded by expert panel discussions about the CDD strategies of Russia and NATO. The exercise was followed by two panels on lessons learned and next steps, to help derive lessons from the TTX.

In keeping with the past two seminars, participants from the United States, allied countries, and international organizations brought their diverse backgrounds in academia, government, industry, the national laboratories, and think tanks to enable a wide-ranging conversation. The participants wide range of specialized expertise, including conventional (sea, air, and land), nuclear, space, and cyber, as well as diplomatic and economic, in order to round out the seminar's focus on cross-domain deterrence linkages and applications to *Diplomatic, Information, Military, and Economic* (DIME) elements of national power.

The first two days took place in an unclassified setting which allowed for full participation of U.S. and international attendees. On the third and last day, classified briefings and discussions were held with allies in the morning, followed by an afternoon U.S.-only session. This seminar report only addresses the unclassified interactions. This report summarizes key points from the a not-for-attribution discussions. Summaries of the previous two seminars are available at https://cgsr.llnl.gov/content/assets/docs/SummaryNotes.pdf (for the 2014 seminar) and https://cgsr.llnl.gov/content/assets/docs/CDD_Seminar_2015_Report.pdf (for the 2015 seminar).

Overview

In the 2016 CDD Seminar, the deterrence community continued its exploration of deterrence challenges in an increasingly dynamic security environment. Indeed, the real-world events of the past year validated many of the findings of prior seminars and in some cases, overtook the scenario planning for the TTX. World events and the insight gained during the TTX challenged participants to come to terms with the realities that

accompany the resurgence of peer and near-peer competitors. This resulted in a consensus view that "deterrence thinking" needs to be renewed and pursued to effectively address the evolving security environments in a more integrated framework.

The lack of progress in determining a practical framework for integrating all the domains into strategic planning was noted, and the "stovepiping" that bedevils integration and the challenges of enabling leaders to make real-time decisions across multiple domains was clearly demonstrated. It was acknowledged that the United States and NATO alliance partners are not yet adept at this integration. Effective application of CDD options within integrated Western operations remains limited. In contrast, however, Russia appears to have made significant progress in integrating across domains, as demonstrated through their strategies evident in Eastern Europe, the Middle East, and Western Pacific. So, a key objective of this year's seminar was to understand the issues surrounding integrating cyber and space domains into the overall framework of cross-domain deterrence. The participation of civilian and military cyber and space experts helped to focus many of the seminar's discussions on the application of cyber and space into the larger deterrence framework.

A key finding was that operationalizing integrated planning, to include space and cyber with input from (whole of government) policy- and decision-makers, is necessary to avoid inadvertent escalation and to improve effectiveness during crises. However, subsequent discussion found that application of cyber and space options, either independently, or in concert with other domains, was not well understood. Two factors resulted in this unclear understanding: (1) continuing challenges of information sharing in what have traditionally been highly classified national security domains; and (2) a general lack of knowledge regarding capabilities that could be applied to the overall deterrence framework. In addition, it was found that the lack of internationally-accepted norms in the cyber and space domains complicates the situation in pre-conflict, transition and conflict conditions. In this regard, inadvertent escalation through unintended consequences of actions in cyber and space was a key concern among participants.

Panel 1— Concept Development for Integrated Strategic Deterrence

This panel focused on how to evolve the understanding of CDD toward a fully integrated approach to strategic deterrence. While U.S. and alliance deterrence thinking continues to evolve, incorporating cyber and space domains into the overall CDD framework remains problematic, largely due to technical knowledge requirements (in the forces) and the classified nature of cyber and space systems, operations, and information. It was noted that at the 2016 Warsaw Summit, NATO formally recognized cyber as an operational domain because of its increasing role in geopolitical and military affairs. However, integration of cyber and space operations with operations in other domains remains challenging due to the difficulties in formulating deterrence policy and the lack of agreed upon international norms of behavior in these new "global commons."

The most effective framework should create more credible response options and increased strategic stability. Participants identified the early application of non-military

levers of power in DIME to respond to adversary provocations in pre-conflict or gray zone phases of operations as a key element of strategic deterrence. However, some cautioned that "blurring the lines of conflict" could lower the threshold for adversary nuclear employment in response to actions outside of the nuclear domain.

The was general consensus on the need for an integrated strategic deterrence framework that addresses thresholds, redlines, and proportional response, while recognizing the differences in adversary perceptions of different U.S./alliance courses of action. Participants supported development of a CDD "toolkit" to provide U.S. and alliance leadership with substantial options to counter adversary aims both in pre-conflict and conflict phases. The importance of understanding integrated deterrence planning that includes cyber targeting of the "economic" sector, especially given recent U.S. emphasis on financial sanctions in response to the annexation of Crimea and other Russia actions (e.g., curtailing oil and gas supplies to Europe) and Russia's use of cyber attacks against Western Europe was stressed.

NATO agreed to strengthen its deterrence posture at both the Wales and Warsaw summits. The 2016 Warsaw decision to forward deploy multinational forces in Eastern Europe with both conventional military and cyber forces shows that NATO is beginning to bring CDD capabilities to bear within a unified alliance construct. However, some participants believed that a deterrence posture based on CDD could make alliance decision-making more difficult and could strain alliance cohesion if there is disagreement on the potential CDD effects. It was observed that the tendency of the United States and NATO to seek the "high moral ground" by constraining actions could be problematic when facing an adversary with no such constraints and recommended further analysis on how to properly counter such unconstrained adversaries. Panelists stressed the importance of strategic messaging and applauded NATO's efforts to increase public awareness to counter Russian gray zone tactics.

Panel 2— Russia's Approach to Integrated Strategic Deterrence in Regional Conflict

Russian military strategists have developed a strategic deterrence paradigm that allows Russia to effectively deter a potential adversary by relying on a range of non-military and military (including nuclear) means. Unlike U.S. and alliance thinking regarding discrete phases of conflict, Russia applies a more continuous view of conflict and appears to be effectively exercising its capabilities all along this continuum.

Some discussions focused on Russian efforts to integrate its capabilities to counter what it perceives as the West's superior conventional forces. Russia's annexation of Crimea, continued aggression in Ukraine, support for Syria, arms buildup in Kaliningrad, and its meddling in U.S. and European elections demonstrate that Russia is successfully applying CDD capabilities in all phases of conflict, including the gray zone.[1]

[1] Gray zone tactics refers to measures that fall below the threshold for traditional armed conflict. Examples include special operations, propaganda and information influence campaigns, and economic sanctions and blockades. Also known as hybrid threats (or warfare)

Russia is deepening the integration of both its force structure (horizontal integration) and capabilities on the battlefield (vertical integration). The latest Russian *horizontal integration* efforts involve: 1) the integration of air forces, air defenses, and space forces into a single unified military command; 2) the continued evolution and use of information warfare that combines electronic warfare, cyber operations, and information operations; and 3) development of counter command and control (C2) capabilities, including anti-satellite (ASAT), deep strike capabilities, and other capabilities to attack communications infrastructure, e.g., undersea fiber optic cable attack.

Russia's annexation of Crimea and subsequent support of Russian-backed rebels in eastern Ukraine remain the best examples of Russian *vertical integration* of capabilities and Russian application of multiple domains of warfare. These actions include the integrated use of special operations (e.g. the surprise use of "little green men"), information warfare (e.g. deception, propaganda, cyber attacks, etc.), and conventional warfare (e.g. use of Russian tanks, missiles and artillery on the battlefield). Russia also applied strategic messaging, including a nuclear messaging campaign in order to prevent the United States and NATO from responding. Thus, Russia exploited gray zone conflict to carefully remain under the threshold for an armed U.S./NATO response, including avoiding potential invocation of NATO Article 5 by the Baltic States. Furthermore, by creating an initial *fait accompli* and holding territory in eastern Ukraine and in Crimea, Russia shifted rapidly to conflict termination to convince others that it was too costly to reverse initial Russian aggression. Panelists stressed that successful and early termination of a limited conflict is critical, as Russia does not desire, and would be unlikely to win, a protracted conflict against a unified NATO.

Panel 3 – The Impact of Cyber and Space Technology

The understanding and application of space and cyber capabilities and their role in CDD is continuing to evolve. Both domains require additional understanding to be effectively applied in an integrated strategic deterrence framework. This is due, in part, to the sensitive (and often highly classified) nature of cyber and space operations and capabilities.

Cyber operations can include cyber network exploitation (CNE) and cyber network attack (CNA). Most current cyber actions are characterized as CNE, such as non-state and state actors seeking unauthorized access to information for the purposes of espionage. Examples of CNA are generally described in terms of destroying networks or seeking access to create kinetic effects and range from traditional distributed denial-of-service (DDOS) attacks to attacks with kinetic effects, such as attacks on electricity generating stations. Attribution and the methods of deterring against both CNE and CNA were important topics. Cyber operations might be deterred by denial (hardening defenses to keep adversaries out of critical networks) or by punishment (either in domain with retaliatory cyber attacks, or out of domain, e.g., through financial sanctions).

While cyber capabilities have a role in the application of so-called soft power operations, cyber operations are more effective when combined with other aspects of information warfare. Discussion concentrated on the more "hard power" aspects of cyber, including how cyber operations can be applied to bolster force projection and delivery of effects prior to conventional military operations. Participants debated the military utility of cyber operations with some arguing that the hardness of military networks and uncertainty regarding the desired effects from cyber operations reduces the utility of cyber operations. Others expressed concern that network-centric warfare increases the vulnerability of our networks to cyber exploitation by our adversaries. There was a robust debate regarding *escalation risks from cyber*. Some participants saw the cyber domain as defense dominant with unclear escalation risks because of the uncertainty of effects, thereby reducing the strategic value. Others saw potential de-escalatory and crisis management benefits from the use of cyber. But cyber soft power operations could also be viewed as potentially highly escalatory and questioned whether adversarial soft power usage without a robust U.S./allied response would embolden adversaries to increase aggression.

Historically, the United States has maintained a significant advantage in space capabilities and operations. Critical U.S. space capabilities include those that provide nuclear command and control, global positioning system (GPS), other intelligence, surveillance, and reconnaissance (ISR) systems. As peer and near-peer states continue to gain both space and counter-space capabilities, the space domain is increasingly competitive and contested and therefore *the escalation risks from space capabilities* need to be considered. To date, U.S. policymakers have not seen the need to field counterspace capabilities. The technological advances in counterspace capabilities, combined with first strike advantages, create major escalation risks, and efforts should be made to increase transparency and develop rules of the road in outer space with an emphasis on crisis avoidance and escalation management.

Panel 4 – Reflections on Lessons Learned from the TTX

The CDD Seminar TTX was designed to challenge and stimulate thinking about CDD and the application of United States (Blue), NATO (alliance), and Russia (Red) domains in a Baltic conflict scenario. The TTX conducted two moves: (1) Explore U.S. and NATO responses to aggression and Russian coercion in a period of rapidly rising military tension but short of actual armed conflict; and (2) Explore U.S. and NATO responses during combat operations to achieve conflict dominance and escalation management following limited Russian nuclear employment aimed at de-escalating the conflict on its terms. Participants were divided into two teams each with domain-specific sub-teams and "whole-of-government" sub-teams. Each team included a Blue and an alliance lead whose job it was to integrate multiple domain-specific possible responses into recommended options for decision makers. Red observers were assigned and did not explicitly act in the TTX, but provided their views of U.S. and alliance deliberations during the TTX out-briefs. The findings and key outcomes from the TTX are summarized below.

Integrating Multiple Domain Response Options

Participants in the TTX observed that deliberate planning of cross-domain strategic messaging campaigns and operations should be done in times of peace before the time urgency of conflict is an issue. Whole-of-government participation in integrated strategic deterrence should be encouraged and options other than "domain-on-domain" responses should be considered and evaluated for effectiveness in crisis management. U.S. and alliance team leaders were challenged to take the recommendations from their sub-teams to formulate response options that bolstered deterrence in the pre-conflict phase or that managed escalation in the conflict phase. The TTX experience of applying an integrated approach illustrated the difficulty of taking the overall CDD goals from the strategic level to an operational framework for use on the battlefield. Participants and senior observers recommended that similar TTX opportunities including U.S. and alliance policymakers could be well used to better explore CDD policy implications and concepts of operations.

Overcoming Perceptions that Undermine Escalation Control and Deterrence

U.S. and alliance civilian and military leadership are rightly concerned regarding responsive actions that might have unintentional escalatory effects. However, adversaries may perceive this wariness as an opportunity to continue provocative activities, especially when in conflict below any established threshold for U.S./NATO response. A seeming lack of alliance political will to engage in military conflict may risk emboldening the adversary to escalate. The TTX illustrated that earlier recognition of the seriousness of pre-conflict adversary behavior and stronger U.S./NATO response (in appropriate domains) could serve to enhance deterrence. U.S./NATO willingness to appropriately respond clearly to Russian gray zone behavior with effective strategic messaging, could change Moscow's decision calculus in a manner favorable to de-escalating the conflict.

Developing proposals for conflict short of war

It was generally agreed that U.S. and alliance messages are most credible when there is a direct and unambiguous threat to the sovereign integrity of an ally and Article V is invoked, and that they are least credible for deterring actions that are coercive or ambiguous in their implications. Developing proposals for U.S./NATO responses in gray zone or conflict short of war proved challenging. Several reasons for this include:

1) Inability to reach a consensus across the diverse NATO member states regarding decisions that some may deem too escalatory (even if such moves were necessary to prepare for future adversary escalation);
2) Desire or self-imposed constraints to follow international norms, even when the adversary is clearly violating these norms; and
3) Over-emphasis on seeking off-ramps, while U.S./NATO forces are suffering from initial combat losses, when the adversary clearly has no intention of backing down.

The group struggled with implications of these challenges, especially given real-world Russian and Chinese actions, short of war, in both Ukraine and the South and East China Seas. Some argued for an alteration in how we think about the stake for U.S. and alliance credibility in gray zone conflicts. This might include rethinking the U.S./NATO linear, discrete phased approach to conflict to increase flexibility of response, including multi-domain response.

Closing Observations

Over the course of three Cross-Domain Deterrence Seminars, the strategic deterrence community's understanding of the definition, integration, and application of multi-domain integrated strategic deterrence concepts has improved and evolved. However, much work remains to incorporate the nascent cyber domain and to properly account for the emerging competition in space into an integrated strategic deterrence framework. Participants agreed that "integrated strategic deterrence" or "multi-domain deterrence" are better descriptors of what we are trying to capture when we talk about the application of all the levers of power at our disposal. In fact, the term "cross-domain deterrence" is falling out of favor, with many suggesting that it is too nebulous a term to be applied in a rigorous fashion for our needs. It would be useful if the domain framework be expanded across the whole-of-government to include information, economic, and diplomatic domains, as well as conventional, nuclear, cyber, and space.

This work was performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under Contract DE-AC52-07NA27344. LLNL-TR-728737